**Cybersecurity**

Many new and emerging issues within the Information Technology field relate to exciting new ways society can leverage new capability to improve progress in business, manufacturing, conservation and many other fields. Within this, Cybersecurity sits as a foundation block to secure private and proprietary data in an increasingly connected and cloud-based world. With the number of interconnected devices expected to reach 24 billion by 2020 (Internet of Things IoT A vision, architectural elements, and future directions)), getting cybersecurity right is a key part of an organisation fulfilling it legal and ethical obligations to those whose data it acts as a steward of.

Rainer Jr and Prince (2016) identify three major types of information security controls – physical controls, access controls and communication controls. With data increasing being hosted on open networks as opposed to heavily secured closed ones of the past (Riahi Sfar et al., 2018), physical security becomes less of a risk factor than perhaps it was in the past, as physical vicinity is no longer as important as it once was.

Access controls relate to ensuring that a data source is being accessed by the correct person, rather than a malicious outsider. Authentication in the early days of the internet consisted of username and password. Single-factor authentication such as this imposes incredible vulnerabilities, as it relies on users selecting a highly complex password and using a unique password for every service they use. With the average user using the same password across approximately four different services (Rainer Jr and Prince, 2016), and the large number of passwords user are prompted to create an enter on a daily basis, poor password choices are seemingly encouraged (Renaud and Zimmermann, 2018). As such, two- or multi- factor authentication greatly strengthen authentication controls as they rely on something the user has (such as a smart card or USB key) and/or does (such as receiving a push notification or security SMS) to complete the log on process.

Communication controls secure the digital movement of information across networks. Encryption and cryptographic protocols sit within this control as the arguably the most relevant topics over the last decade. Indeed, multiple security issues have been publicised over the last decade affecting cryptographics. Perhaps the most infamous of these is the HeartBleed vulnerability discovered in the OpenSSL library in April 2014, which allowed a malicious TLS heartbeat request to return large amounts of buffer memory, potentially containing sensitive user information and passwords (Synopsys Inc, 2014). Of particular concern is that the patch for this vulnerability largely resulted in a net line change of only 2 lines of code, putting the vulnerability itself down to a simple logic error (Harris, 2018).

The recent and ongoing implementation of Transport Layer Security (TLS) 1.3 brings massive changes to the protocol as it widely implements a concept known as Perfect Forward Secrecy (PFS) (Rescorla, 2018). The use of PFS ensures that if a user’s encryption key is compromised, a malicious outsider is unable to access and decrypt further information from the webserver, whether it relates to the compromised user or not.

The ongoing development within the cybersecurity field is a boon for system administrators, businesses and end users alike. With the supercession of legacy and weaker methods of security, such as single factor authentication, and vulnerable cryptographic protocols, private and proprietary data is likely to be more secure from malicious outside access. Of course, any protocol is only as strong as its implementation, so the need for highly skilled security engineers is likely to continue long into the future. In turn, this is likely to change the vectors of attack by malicious outsiders from intrusion type attacks, as these will be easier to detect and defeat in the future. This has already been seen within the banking industry, where increased detection and monitoring capabilities have seen a shift from malicious attacks toward social engineered and scam-related compromise vectors. According to the latest scam statistics (Australian Competition and Consumer Commission, 2019), monetary loss relating to scams and phishing is on trend to grow in 2019 by up to 25%, far outstripping the grow rate in previous years. It is difficult to detect such events as they are primarily established users exhibiting an unexpected behaviour in their authorised access rather than a malicious outsider attempting to force access to a resource or data. As such, the importance of training of employees and the wider public to the danger of such events is key, and is likely to be of huge importance moving forward. Organisations are increasingly turning to phishing simulation emails, where a company, or an outside firm acting on behalf of the company, sends an email which appears to be a phishing email to a large number of users. If a user clicks on such an email, they are taken to a page which advises them they have clicked a phishing email, and data is captured on who has responded to the phishing email. Despite this increase in training and awareness, data suggests up to 20% of employees are still responding to phishing emails, simulated or real (Williams et al., 2018), which shows there is a long way to go on this.

As for everyday users and consumers, technological developments, if implemented correctly, may see them less at risk of their data being accessed through an organisation’s servers or databases without their or the organisation’s knowledge or consent. However, as mentioned above, the onus may fall more on the consumer to ensure they are securing their own data. Regardless of their intention, when user responds to a phishing email, or provides a payment due to a false invoice they have received, they are actively participating in the compromise of their own data or finances. As such it is more important than ever for users to be mindful of where and with who they are sharing their personal details and security credentials, and to also make sure they are engaging in independent research before making a financial or data commitment.

References

AUSTRALIAN COMPETITION AND CONSUMER COMMISSION. 2019. *Scam statistics* [Online]. Available: <https://www.scamwatch.gov.au/about-scamwatch/scam-statistics> [Accessed 29/09/2019].

HARRIS, J. 2018. HEARTBLEED: A CASE STUDY. *Issues in Information Systems,* 19.

RAINER JR, R. K. & PRINCE, P. 2016. *Introduction to Information Systems : Supporting and Transforming Business,* Hoboken, John Wiley & Sons, Inc.

RENAUD, K. & ZIMMERMANN, V. 2018. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy***,** 1-31.

RESCORLA, E. 2018. *The Transport Layer Security (TLS) Protocol Version 1.3* [Online]. Internet Engineering Task Force. Available: <https://tools.ietf.org/html/rfc8446> [Accessed 29/09/2019].

RIAHI SFAR, A., NATALIZIO, E., CHALLAL, Y. & CHTOUROU, Z. 2018. A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks,* 4**,** 118-137.

SYNOPSYS INC. 2014. *Heartbleed Bug* [Online]. Available: <http://heartbleed.com/> [Accessed 29/09/2019].

WILLIAMS, E. J., HINDS, J. & JOINSON, A. N. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies,* 120**,** 1-13.